SECURE COALITION ID
Protecting Identity with Technology

May 5, 2011

Honorable Sam Johnson
Chairman
Committee on Ways & Means, Subcommittee on Social Security
House of Representatives
Washington, DC 20515

Dear Chairman Johnson:

On behalf of the Secure ID Coalition (SIDC), I am pleased to submit the following comments as follow-up to the Subcommittee Hearing held on April 14, 2011 titled *Social Security Administration's Role in Verifying Employment Eligibility.*

During the course of the hearing, you asked witnesses about the use of biometric data for ID authentication in systems deployments. It was clear from the responses the witness provided that they had limited experience with the deployment and operations of biometric based programs and how expertise of such programs could be applied to the area of E-Verify. The SIDC submits these comments in an effort to dispel the misconceptions held by the panelists and provide factual information about how biometrics can be used for identity authentication as part of the E-Verify program.

First, it is important that we address the question of security of biometric and card-based systems. Statements made at the hearing with respect to biometric card deployments that questioned the security of chip-based identity card systems, also known as 'smart cards', suggesting they were easily hacked "in a matter of hours." This statement is not factual and our industry would like to see the data from the hacking incident referenced by Director Stana of the General Accounting Office.

The truth is that smart card technologies combined with biometrics are considered the 'gold standard' of identity management security, and are used both here and globally to provide the utmost in security, privacy and system performance. The U.S. government has already implemented biometric smart cards in numerous applications requiring the highest security, including the Department of Defense Common Access Card (CAC), the U.S. FIPS 201 Personal Identity Verification (PIV) Card, the U.S. Transportation Worker Identification Credential (TWIC), and the Electronic Passport. Other examples include the Singapore Immigration Automated Clearance System, the Canadian Airport Restricted Area Identification Card, Amsterdam's Schiphol Airport, and the University of Arizona Keyless Access System

Card. All of these applications reference above have been used for years with the highest degree of system integrity and success.

Cost concerns were also raised in the hearing regarding the implementation of biometrics into the E-Verify system, based on anecdotal evidence from the TWIC program. It should be noted that the deficiencies found in the TWIC program are the results of poor oversight and insufficient program planning and management, not failures in the technology. The SIDC would like to refer to the Committee the GAO's September 2006[1] and November 2009[2] reports on the TWIC program as a chronicle to this point.

If the U.S. government were to implement a worker ID and authentication credential that incorporates biometrics, the actual costs would most likely be modest. In the existing applications mentioned above, the lion's share of costs incurred has not to do with the technology itself, but with the vetting process required by the issuing organizations. As one would imagine, the Department of Defense's Common Access Card requires an extremely high level of assurance that the person being issued the card is who they claim – a level that requires numerous background and security checks. Because of the secure nature of what the card would grant access to – our most sensitive national defense systems – there are a number of additional security measures built into the card, such as anti-tamper technologies, microprinting, and holograms, to name a few. Understandably, these precautions increase the cost of the card, but through a risk-based analysis, the costs are well worth being borne.

Applying the same risk-based analysis to a proposed worker credential, the level of vetting and anti-tamper precautions would be significantly lower because the risk is lower. A worker identification card would certainly have to incorporate technologies to ensure against tampering or counterfeiting, but these would be inexpensive as the security would be built into the smart card's microcontroller and the card form itself can take advantage of existing off-the-shelf anti-counterfeiting measures currently used by those who issue drivers' licenses.

Further cost reductions can be achieved through the architecture of the system. Deploying a biometric card based process for E-Verify would allow the employer to verify the employee without having to be linked to back-end database – the source of a large amount of costs due to the security required. For the purposes of creating a secure, reliable and scalable E-Verify program, SIDC would propose a contact based card solution that would contain a secure chip; these smart cards have been proven secure and cannot be duplicated, skimmed or spoofed. Information stored on the secure chip could include name, account reference information and biometric template. Such an approach would allow the biometric to be compared with the template stored on the card without using an online database.

[1] U.S. Government Accountability Office. (September 2006). *Transportation Security: DHS Should Address Key Challenges before Implementing the Transportation Worker Identification Credential Program.* (Publication No. GAO-06-982).

[2] U.S. Government Accountability Office. (November 2009). *Transportation Worker Identification Credential: Progress Made in Enrolling Workers and Activating Credentials but Evaluation Plan Needed to Help Inform the Implementation of Card Readers.* (Publication No. GAO-10-43).

Additional concerns were raised about the collection and storage of worker information, both from a civil liberties and a privacy vantage point. By operating without a back-end database as mentioned above, civil liberty and privacy concerns can be addressed. In the SIDC's proposed system outlined below, only the federal government would collect and store a worker's biometric – as would be necessary for maintaining a reference data set and ensure no one has enrolled twice. This database would be secure and encrypted, and to further protect worker privacy in case of breach, personal information should be held in a database separate from the actual biometrics. Further, these databases should not be allowed to be accessed by the public, and only to those government officials authorized to by law. Citizen concern over the use of the biometric by the government for unintended uses (i.e., those not linked to worker authentication) can be ameliorated by implementing strong civil and criminal prohibitions in the authorizing legislation.

Personal privacy is further protected because the employer would not have access to the government database. Since the worker's biometric would be turned into a template (a computational representation of the biometric) which is then placed on the smart card's chip, the actual biometric is never at risk of being lost. Further the card, and as such the biometric, is carried and controlled by the cardholder not the employer. The employer's card reader would compare the biometric template on the card with the live biometric presented by the worker. If the biometric matches the template on the card that was presented at enrollment, then the worker is approved. At no time would the E-Verify software allow the employer to collect or store the employee's biometric. The only information that would be sent back to the E-Verify program would be whether or not the employee's biometrics matched.

Below is an overview of how such a system might be deployed for E-Verify

- The process would start with a letter from the Social Security Administration to the address of record for the individual (much like the annual Social Security statement previously sent to workers each year).
- The letter would include an individual code which would NOT be the Social Security number (SSN). This code would be a 'cryptographic hash', a mathematical cipher of data including name, address or region, and SSN.
- Each individual's code would be unique and associated with a Social Security record. The letter could only be validated with the correct Social Security number which would need to be provided by the individual. Therefore if the letter was intercepted, the interceptor would also need to also know the SSN associated with the letter and record.
- The letter would offer a reasonable time frame (maybe two weeks to a month) for the individual to come to an enrollment center convenient to them (i.e. their local post office or nearest federal building) to upgrade their Social Security card. The letter would also include the address of the enrollment center facility.
- The individual would be required to bring the letter (with the code) and other supporting documents to facilitate the Social Security card upgrade. At the enrollment center, the individual would provide the letter (something they have) and the associated SSN (something they know) and other documentation (maybe two forms of ID, with one having a photo). The Social Security record would be inaccessible to the enrollment center unless the letter with the correct code is presented.

- At the time of enrollment, the individual would have their biometric (such as a fingerprint, iris pattern, or hand geometry) scanned and enrolled in the system.
- The system would then check the newly scanned biometric against the enrollment database. If the biometric has not been seen before by the system, then the individual account is updated with the newly enrolled biometric. The biometric would then be associated with that individual record. If the biometric is already in the system, then the individual would be sent through a redress process.
- The individual would be issued a new chip-enabled electronic Social Security card that would incorporate the necessary security features and be tamper resistant. The chip would store the information usually found on the front of the legacy Social Security card (name and SSN) as well as a template of the individual's biometric. This ensures the individual's personal privacy as their actual biometric is never stored on the card, just a computational representation of the biometric.
- Upon hire the worker would present the new electronic Social Security card to the employer. The employer would insert the card into the reader and ask the new hire for their corresponding biometric. The reader would determine if the biometric presented by the new hire matches the one presented at the time of enrollment. The employer would immediately receive a green light for 'YES' or a red light for 'NO', as well as a receipt for both the employer and the employee.
- If the system responds YES, the employer is then free to engage the employee as they are now able to show they successfully completed the process. If the system responds NO, the prospective new hire would need to go through a secondary confirmation process.

This outline is merely a rudimentary sketch of how such a system could work for E-Verify, but should give the Subcommittee ideas of where privacy and security can be architected into the system, and how costs can be maintained at an acceptable level.

Thank you for the opportunity to submit comments to the Subcommittee regarding the April 14, 2011 hearing on E-Verify. The Secure ID Coalition would be pleased to serve as a resource to the Subcommittee as they evaluate how to further secure the E-Verify system. Please feel free to contact me directly at kemerick@secureidcoalition.org or 202-464-4000.

Respectfully Submitted,

Kelli A. Emerick
Executive Director